SECRET

DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

SECOM-D-245

7 December 1983

MEMORANDUM FOR: Deputy Director, Intelligence Community Staff

25X1 FROM: [redacted]
Chairman

25X1 SUBJECT: Proposed SECOM Response to DCI Request [redacted]

1. Attached for your approval is a proposed response to the DCI's 28 November 1983 memorandum, requesting additional information about SECOM's
25X1 status report to him. [redacted]

2. The DCI's offer to weigh in on the leak problem is gratifying, but the risk at this time of unfavorable publicity seems to outweigh the likeli-
25X1 hood of positive results. [redacted]

3. The request for the comparison of PD-24 and the proposed NSDD on communications and computer security probably can be fulfilled best by providing the IC Staff's 28 October 1983 input to the DDCI. Subject to your approval, I have included that document as an attachment to the SECOM
25X1 response. [redacted]

25X1 [redacted]

Attachment

Regraded CONFIDENTIAL When
Separated from Attachment

CL BY SIGNER
DECL OADR
DERIVED FROM MULTIPLE

WARNING NOTICE - INTELLIGENCE
SOURCES OR METHODS INVOLVED

SECRET

25X1

SUBJECT: Proposed SECOM Response to DCI Request [redacted]

Distribution:
1 - Addressee w/att
1 - ICS Registry w/att
1 - SECOM Subj w/att
1 - SECOM Chrono w/att

SECRET

DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

SECOM-D-243
7 December 1983

MEMORANDUM FOR: Director of Central Intelligence

VIA: Deputy Director of Central Intelligence
Director, Intelligence Community Staff

25X1 FROM: [redacted]
Chairman

25X1 SUBJECT: Security Committee Activities [redacted]

REFERENCE: DCI Memorandum to C/SECOM, dated 28 November 1983

1. In your response (Reference) to the Security Committee's recent status report, you asked (a) how prior DCI's have weighed in on the leak problem and (b) to see the comparison of PD-24 and the proposed NSDD on
25X1 communications and computer security. [redacted]

2. Regarding leaks, you have exceeded by a considerable margin the efforts of the other DCI's to weigh in on the problem. The videotape you made in June is being shown around the Community and is being favorably received. Because of severe current press criticism of Administration anti-leak efforts, it is unlikely that putting the DCI's prestige on the line at this time would serve a useful purpose. Your continued support of FBI investigation of specific leaks, however, could bring positive
25X1 results. [redacted]

3. The effort to replace PD-24 with a single NSDD covering both communications and computer security has been overtaken by events. The IC Staff input to the DDCI on this matter, including the SECOM comparison you requested, is attached. A draft replacement for PD-24, concerning only
25X1 COMSEC, has been prepared and is being reviewed in the Community. [redacted]

25X1 4. Please advise if further information is desired. [redacted]

25X1 [redacted]

Attachment

Regraded CONFIDENTIAL When
Separated From Attachment

CL BY SIGNER
DECL OADR
DERIVED FROM MULTIPLE

WARNING NOTICE - INTELLIGENCE
SOURCES OR METHODS INVOLVED

SECRET

25X1 SUBJECT: Security Committee Activities [redacted]

Distribution:
Orig - Addressee w/att
1 - DDCI w/att
2 - ER w/att
1 - D/ICS w/att
1 - ICS Registry w/att

DCI/ICS 83-4044
28 October 1983

MEMORANDUM FOR: Deputy Director of Central Intelligence

25X1 FROM: [redacted]
Director, Intelligence Community Staff

SUBJECT: Concern Relating to the Proposed Revision of PD/NSC-24

1. A proposed revision to PD/NSC-24 (Telecommunications Protection Policy) has been formulated by Ken deGraffenreid of the NSC and selected members of the National Communications Security Committee (NCSC). The revision is based on the findings of the Countermeasures Organization Study produced under the auspices of the Senior Interagency Group (Intelligence) in July 1983 in response to NSSD-2. Under this revision, PD/NSC-24 will be entitled "National Policy on Telecommunications and Automated Information Systems Security"--a significant expansion in the scope of activities covered. This memorandum highlights the concerns and comments expressed by the IC Staff, CIA/OC, and CIA/OGC regarding the proposed revision. Attachments 1, 2, and 3 (which were developed by the DCI's Security Committee, CIA/OC, and CIA/OGC, respectively) provide comparisons of the proposed NSDD
25X1 with the present PD-24. [redacted]

2. All parties are agreed that there is a need for national policies for the protection of telecommunications and automated information systems. The proposed revision would establish a single national policy and management structure covering both disciplines. Although there is philosophical agreement that separate policies might leave gaps in the protection of information as the technologies of the two disciplines converge, concerns were raised over the feasibility of managing a consolidated effort, particularly in view of the expanded scope of the systems addressed in the current proposal.
25X1 [redacted]

3. The proposed NSDD identifies the Secretary of Defense as the Executive Agent of the Government for Telecommunications and Automated Systems Security. There is some concern within the IC Staff and CIA/OC over the appropriateness of having the Secretary in this role because the proposed NSDD
25X1 expands security to include information affecting privacy of US persons. Several other related concerns are identified in the attachments. [redacted]

4. There is unanimous concern that the proposed NSDD does not accurately recognize the DCI's statutory responsibilities and authorities. Several actions in particular in the proposed NSDD could severely impact the DCI's ability to carry out his responsibilities. These include:

This memo is downgraded to CONFIDENTIAL upon removal of attachments.

WARNING NOTICE
INTELLIGENCE SOURCES
OR METHODS INVOLVED

CL BY SIGNER
DECL OADR
DERIVED FROM MULTIPLE

a. The development of a consolidated resources program and budget proposal for national telecommunications and information systems security, which could both dilute the DCI's responsibilities regarding formulation of the NFIP and impact Intelligence Community priorities.

b. An implication that DIRNSA, who is designated as the National Manager for Telecommunications and Information Systems Security, assumes authority for the security accreditation both of government and contractor telecommunications and information systems, thereby possibly impacting adversely on the DCI-authorized missions of CIA/OC/COMSEC and CIA/OS/ISSG.

c. An implication that DIRNSA has sole responsibility for assessing and disseminating information on hostile threats to telecommunications and automated information systems, thereby removing related analytic missions from FBI, CIA, and DIA.

d. A requirement that DCI provide DIRNSA with "unique handling requirements associated with the protection of sensitive compartmented intelligence" and an implication that DIRNSA could accept, modify, or reject the DCI's requirements without regard to the DCI's statutory responsibilties and authorities. 25X1

5. All the concerns identified in the attachments should be addressed by the originators before the NSDD is promulgated. An alternative mechanism for accomplishing the actions identified in the NSDD must be developed which does not supplant the responsibilities and authorities of the DCI and other government executives identified in the draft. 25X1

6. A revision of the NSDD which places the responsibility and authority of the DCI and other government executives in proper perspective may make an umbrella national policy feasible. DIRNSA already has COMSEC responsibilites for the US Government. Department and agency heads presently carry out their respective COMSEC missions under the procedures and policies jointly developed under the auspices of the NCSC. DIRNSA, as the Executive Agent for the DOD Computer Security Evaluation Center (CSEC), currently is also responsible for generic computer security R&D, systems evaluation criteria, and preparation of and budgeting for the "DOD Consolidated Computer Security Program," which encompasses reporting of CSEC and all other DOD branches and agencies' activities in computer security. CSEC does not have computer security responsibilities outside of DOD. 25X1

7. In the proposed PD/NSC-24, DIRNSA would assume government-wide responsibilities for COMSEC and automated information systems security. The unique responsibilities of this new national role require a direct interface between DIRNSA and the Executive Agent. 25X1

8. There is concern about the possible impact of SECDEF delegating his responsibilities under this NSDD through DIRNSA to the newly established DOD Computer Security Center or the NSA COMSEC organization. Such a decision would heighten existing fear that DIRNSA, who manages the two organizations separately, would not be able to deal with the situation in an equitable fashion. 25X1

9. It is recommended that:

- o an official DCI response to this proposed NSDD be developed by the IC Staff in coordination with CIA/OGC, CIA/OS/ISSG, and CIA/OC;
- o the existing policies promulgated under the NCSC remain in effect until the draft NSDD has been revised to address the concerns stated in this memorandum;
- o the new draft NSDD be properly staffed with the agencies under the existing NCSC; and

25X1

- o that progress be deliberate so as to allow incorporation of the results of the DCI's Computer Security Project.

25X1

Attachments: a/s

SUBJECT: Concern Relating to the Proposed Revision of PD/NSC-24

Distribution:
Orig - DDCI
1 - Executive Registry
1 - Office of General Counsel
1 - D/OC
1 - D/OS
1 - SECOM
1 - D/ICS
1 - D/PPS
1 - ICS Registry
1 - IHC Subject (LGS)
1 - IHC Chrono

25X1 ICS/IHC/ [redacted] (28 Oct 83)

COMPARISON OF PROPOSED NSDD WITH PD-24

NSDD	PD-24	CHANGE	CONSEQUENCES
General	General	Expands scope to include all automated systems including word processors.	Raises questions of feasibility of managing consolidated effort.
1	2	Expands security mission to include information affecting privacy of U.S. persons.	Raises questions of Executive Agent's and National Manager's suitability to represent entire Government's privacy interests.
2c, 6b	2c,d	Adds provision for the Government to formulate strategies and measures for providing protection for "systems which handle nongovernment information the loss of which could adversely affect the national interest or the rights of U.S. persons...." Explicit responsibilities and mechanisms to implement this policy are not provided but must devolve on the DIRNSA.	The propriety of this goal, and its pursuit by a military agency, are legal issues which should be explored by the Attorney General.
3	4	Replaces PD-24-based National Communications Security Committee with a Steering Group and National Telecommunications and Information Systems Security Committee (NTISSC).	The breadth of issues covered raises questions of who should be represented on these groups, and what other organizations are affected.

COMPARISON OF PROPOSED NSDD WITH PD-24

NSDD	PD-24	CHANGE	CONSEQUENCES
3c	no ref.	Empowers Steering Group to approve "consolidated resources program and budget proposals" for national telecommunications and information systems security.	Restructures budget review process for these areas, with significant impact on DCI role for NFIP and on department and agency head authorities to set priorities.
3d	4g	Centralizes review of systems' security status by the Steering Group.	Implies migration of accreditation approval responsibilities from departments and agencies to the Steering Group, which would be separated from the environment to be accredited.
4b(3)	no ref.	NTISSC to "administer matters pertaining to the release of sensitive security information, techniques and materials to foreign governments or international organizations (except in intelligence operations managed by the Director, Central Intelligence Agency)."	Supersedes the DCI's E.O. 12333 authorities to prescribe policies for and coordinate foreign intelligence relationships (except for DDO operations).
5	4c	Makes SecDef Executive Agent for Automated Systems Security as well as for Telecommunications Security. Expands his executive agent role to cover all electronic information, not just "national security" information as before.	Considering the rapid expansion of word processing, makes SecDef Executive Agent for all Government information processing.

COMPARISON OF PROPOSED NSDD WITH PD-24

NSDD	PD-24	CHANGE	CONSEQUENCES
5	4d	Secretary of Commerce out as Executive Agent for unclassified, non-national security information, and for commercial and private sector information.	Severely curtails Bureau of Standards role and functions. Raises question of legal propriety of military responsibility for this area.
5f	no ref.	Empowers SecDef to "procure for and provide to government agencies, and where appropriate, to private institutions (including Government contractors) and foreign governments, equipment and other materials."	GSA, and department and agency heads with delegated authority, would lose the right to procure computers and word processors. Centralized procurement would make it very difficult to meet schedule and individual agency requirements.
5g	no ref.	Empowers SecDef to develop and submit a National Telecommunications and Information Systems Security Program budget, "including funds for the procurement and provision of equipment and materials" Government (and contractor) wide.	Seriously affects the budget cycle, department and agency head administrative prerogatives, and DCI role in NFIP. Raises questions of feasibility of discharging this responsibility.
6	no ref.	The DIRNSA would be responsible for carrying out the foregoing responsibilities of the Secretary of Defense as Executive Agent.	All previously itemized SecDef responsibilities may be delegated to DIRNSA.
6a,e	no ref.	Empowers DIRNSA to "empirically examine Government telecommunications and automated information systems and evaluate their vulnerability to hostile interceptions and exploitation."	Shifts security accreditation responsibility for all Government and contractor telecommunications and information systems to DIRNSA.

COMPARISON OF PROPOSED NSDD WITH PD-24

NSDD	PD-24	CHANGE	CONSEQUENCES
6b	no ref.	Empowers DIRNSA to develop and approve "all standards, techniques, systems and equipment" "related to cryptography, communications security and trusted computer and automated information systems."	Entire Government must use DIRNSA specified standards, techniques, systems and equipment.
6b,e	no ref.	Empowers DIRNSA to perform all Government-sponsored R&D for telecommunications and information systems	Eliminates such roles for CIA (ISSG and ORD), DOE (LLL, etc.), Bureau of Standards, GSA and others.
6b,10a	4g	Removes PD-24 authority of heads of Federal departments and agencies to organize and conduct their communications security and emanations security activities as they see fit, and vests this responsibility with the DIRNSA.	In CIA, for example, removes OC COMSEC and OS ISSG missions.
6b	no ref.	Empowers DIRNSA to conduct liaison with foreign governments and international organizations.	Impacts formal and informal roles of DCI, State Department and Commerce Department in many relationships.
6b	no ref.	Empowers DIRNSA to conduct all security-related liaison with private institutions.	Removes Bureau of Standards role with American National Standards Institute, Question of legal propriety arises again.
6c	no ref.	Empowers DIRNSA to operate industrial facilities to provide "cryptographic and other sensitive security materials or services."	Precludes any other agencies from working or contracting in those areas. Could impact private sector research into security methods.

COMPARISON OF PROPOSED NSDD WITH PD-24

NSDD	PD-24	CHANGE	CONSEQUENCES
6d	no ref.	Empowers DIRNSA to assess and disseminate information on hostile threats to telecommunications and automated information systems.	Removes analysis missions from CIA and DIA, such as technology transfer and Soviet technology.
6g,10b	no ref.	Requires department and agency heads to provide DIRNSA all information "he may need to discharge the responsibilities assigned...."	DIRNSA specifies what he wants; others have to provide.
7	no ref.	Requires DCI to provide DIRNSA with "unique handling requirements associated with the protection of sensitive compartmented intelligence."	DIRNSA free to accept, modify or reject requirements. Does not accurately recog- the DCI's statutory responsibilities and authorities.

NSC/PD-24		
1. Established the national policy for the protection of telecommunications ONLY.	1. Expanded to include Automated Information Systems	1. The implementation of the proposed NSDD by departments/agencies (Treasury and Energy for example) where all information handling systems (including telecommunications) are under centralized management will have minimum impact. The other civilian and military organizations will have difficulty implementing the proposed NSDD because of the diversified management of telecommunications and automated information systems. Within the Agency, OC is responsible for telecommunications and the automated systems used in support of telecommunications. ODP and OS/ISSG are responsible for the security of the remainder of the automated information systems.
2. The secretary of Defense was designated as the Executive Agent for Communications Security (COMSEC) (para 4.c). The National Communications Security Committee (NCSC); chaired by the Assistant Secretary of Defense for Communications Command, Control and Intelligence; was established as a national COMSEC framework for the conduct of COMSEC activities within the Government. NSA was a voting member of the NCSC and the charter functions of NSA were clearly defined.	2. The Secretary of Defense is designated as the Executive Agent of the Government for Telecommunications and Automated Systems Security. The Director, National Security Agency is designated as the National Manager for Telecommunications and Information Systems Security and is responsible for carrying out the responsibilities for the Secretary of Defense as Defense as Executive Agent. The NCSC is replaced by the National Telecommunications and Information Systems Security Committee with an expanded membership. A Steering Group consisting of the Secretary of Defense, the Director of Central Intelligence, the Director of OMB, and chaired by the Assistant to the President for National Security Affairs is established to oversee the implementation of the NSDD.	2. Under PD-24 the Director, NSA was a coequal with nine other regular members of the NCSC. With the chairmanship of the NCSC at the AsstSec Def level NSA could not unduly influence national standards or priorities. Under the proposed NSDD the Director of NSA will have a predominant role in determining the future of telecommunications and automated information systems utilization within the Government. The designation of the Director, NSA as the National Manager for Telecommunications and Information Systems Security should be stricken from the proposed NSDD. This is a significant reduction in the authorities of the DCI.

CONFIDENTIAL

NSC/PD-24

3. Provided for "a permanent interagency group, under the chairmanship of the Department of State, be established consisting of representatives of the Executive Office of the President, the Director of Central Intelligence, the Department of Defense, National Security Agency and the Department of Justice/Federal Bureau of Investigation to review and if necessary to deny real estate acquisitions through lease or purchase by the USSR and other Communist countries that present a potential serious threat to U.S. telecommunications security. All foreign government leased or owned facilities in this country should be evaluated as to their possible use for intercept operations."	3. The only mention of this group is contained in paragraph 13 "Responsibility for the Interagency Committee On Real Estate Acquisition is transferred to the Office of Foreign Missions pursuant to PL 97-241, 24 August 1982."	3. The thrust of PD-24 was to reduce or eliminate the vulnerability of unclassified information being passed via microwave and to ensure that classified or unclassified but sensitive information was protected by adequate cryptographic systems. This thrust is lost in the proposed NSDD.
4. PD-24 did not specifically address automated information systems.	4. Automated information systems are incorporated into the proposed NSDD without adequate definition of what is to be covered (computers, word processors, etc.). There are oblique references to a security architecture for systems without any specifics.	4. There are a number of interagency committees that are concerned with computer security under the auspicies of SECOM and the Department of Defense. If the proposed NSDD is approved, Director, NSA will be responsible for all systems. NSA has not demonstrated an expertise in this field.
5. PD-24 very obliquely addresses threat assessments.	5. The proposed NSDD is very specific on threat assessments and tasks heads of departments and agencies to provide any information requested by NSA to determine the vulnerability of telecommunications and automated information systems.	5. The exceptions under paragraphs 7 and 11 are not adequate to resist Director, NSA tasking.

NSC/PD-24 Draft NSDD Revised

6. Paragraph 4.g states that "the heads of all departments and ageancies of the Federal Government shall organize and conduct their communications security and emanations security activities as they see fit subject to the provisions of law, the provisions of this and other directives..."

6. Paragraph 6.a states that as the National Manager for Telecommunications and Information Systems security the Director, NSA shall "empirically examine" government telecommunications and automated information systems and evaluate their vulnerability to hostile interception and exploitation.

Paragraph 11.b states that "nothing in this directive shall give the NTISSC, the Secretary of Defense, or the Director, National Security Agency authority to inspect the personnel or facilities of other departments and agencies without the approval of the head of such department or agency, nor to request or collect information concerning their operations for purposes not provided for herein."

6. Although the wording of paragraph 11.b would imply that the Director, CIA could deny Director, NSA access to CIA facilities to "empirically examine" our telecommunications and automated information systems and evaluate their vulnerability to hostile interception and exploitation, it has been our experience that NSA is very aggressive in pursuing this objective. The finalization of the MOU with NSA on the interface of the CIA secure phone system with the NSA system was delayed several years because NSA insisted on the right to inspect the Agency system for compliance with NSA directives. The revision of DCID-1/16 also contains language that would permit NSA to inspect our telecommunications network to ensure compliance with NSA standards. NSA is unwilling to accept certification from the Director, CIA that the Agency is in compliance with national standards without an "empirical examination."

The original draft of the NSDD contained the following language in paragraph 11.b: "Nothing in this directive shall give the NTISSC, the Secretary of Defense, or the Director, National Security Agency authority to inspect the personnel, facilities, or internal operations of other departments and agencies without their approval." This wording was changed at the insistence of the Agency representative to the working group that prepared the proposed NSDD to ensure that any request by Director, NSA to inspect Agency facilities was addressed to the Director, CIA rather than some unnamed operating official, who might not appreciate the implications of such a request.

28 October 1983

MEMORANDUM FOR: Director, Planning and Policy Staff
Chairman, Security Committee

25X1

FROM: [redacted]
Assistant General Counsel

SUBJECT: Proposed Revision of PD-24,
Telecommunications Protection Policy

1. At your request, I have reviewed a proposed NSDD entitled "National Policy on Telecommunications and Automated Information Systems Security." As we have discussed, it does not appear that there are any strictly legal problems that would preclude adoption of this proposed revision. Rather, the NSDD raises policy issues that, depending upon ultimate resolution, appear to conflict with existing authorities and responsibilities of the Director of Central Intelligence on the protection of intelligence sources, methods, and activities.

2. In my view there are two major issues that must be addressed in preparing a briefing package for the DDCI on the proposed NSDD. The first is the appropriateness of combining telecommunications security and automated information systems (i.e. computer) security under a single national policy umbrella. Part of this issue involves the selection of an appropriate executive agent, and the proposal contemplates that the Director, National Security Agency, will be designated. While this appears to be a case of the tail wagging the dog, there may be no equities of the Director of Central Intelligence at stake.

3. The second major issue is the extent to which the authorities and responsibilities of the Director of Central Intelligence will be subject to the requirements established under the NSDD. Under E.O. 12333 the DCI is responsible to the President and NSC for the security of intelligence systems, and under E.O. 12356 he is responsible for creating intelligence special access programs. Currently DCI security policy requires U.S. Government departments and agencies that process or store intelligence information in automated data processing systems to establish and maintain a formal ADP security program to ensure adequate protection of intelligence information.

25X1

SECRET

(The DCI has issued a computer security manual prepared by the DCI's Security Committee to establish these computer security requirements.) The proposed NSDD could directly affect these DCI responsibilities. For example, section 5 provides that the Secretary of Defense shall provide minimum security standards and doctrine, procure equipment to accomplish the objectives of the NSDD, and develop a consolidated program budget each fiscal year. Moreover, the NSDD does not clearly respect the DCI's responsibilities for intelligence liaison, as section 4(b)(3) provides for a committee, the NTISSC, to administer matters pertaining to the release of sensitive security information, techniques and materials to foreign governments (except in intelligence operations managed by the DCI), and section 6(b) provides that the Director, NSA, is the focal point for conducting liaison with foreign governments. These provisions, if approved without change, would affect the role of the DCI for the protection of intelligence sources and methods, including liaison with foreign governments. (Admittedly, the NSDD recognizes DCI's equities in liaison activities, but falls short, I believe, of providing a complete exemption.) That the draft contemplates a diminished DCI role is further evidenced in section 7 which provides that the DCI shall identify to the NTISSC and the Director, NSA, any unique handling requirements associated with the protection of sensitive compartmented intelligence. The implication is that NSA will have the final word in resolving disputes.

4. In advising the DDCI you may wish to consider a dramatic departure from the scheme that has been proposed in the NSDD. For example, it might be appropriate to establish a senior policy body, such as the steering group that has been proposed, that would include the DCI, the Secretary of Defense, the Director, OMB, and that would be chaired by the Assistant to the President for National Security Affairs. The President could establish a very general national policy but recognize that, as with U.S. National Space Policy, there are three distinct interests that must be served: national defense, civil, and intelligence. Each of these areas could be governed with some degree of independence so long as subject to the overall U.S. policy. While, perhaps, an executive agent would have to be appointed, there would nevertheless remain a clear role for each of these elements to operate in a compartmented fashion, thus preserving the integrity of intelligence processes and requirements while, through the national policy group, attempting to deal with the increasing inter-dependence of these areas. While I do not have any particular thoughts on how these three different systems could be managed at this time, I suggest the NSDD on national space policy could provide an appropriate model from which to begin discussions. I suggest also that thought be given to any need to address this

proposed NSDD in the context of NSDD-97, "National Security Telecommunications Policy", which provides for continuity of government and essential functions during wartime.

5. Clearly a balance must be struck between establishing a consistent national approach to these matters and insuring appropriate protection for intelligence equities. The difficulty in accomplishing this objective arises from the fact that, while intelligence interests generally suggest a compartmented approach, there inevitably is overlap between intelligence and non-intelligence systems. However, a resolution of these issues depends not so much upon legal as policy concerns. Please do not hesitate to contact me if you have any questions or comments.

25X1